

AMENDMENTS TO THE CLAIMS

This Listing of Claims is provided for the convenience of the Examiner; no amendments are being made to the claims.

Listing of Claims:

1. (Previously Presented) A system, comprising:
an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encrypting capability and the remainder having no encrypting capability, the encryption apparatus to perform an encrypting process or a decrypting process on data to enable encryption-based security between those of the plurality of communications terminals having encrypting capability and those of the plurality of communications terminals having no encrypting capability; and
a manager terminal to input information into the encryption apparatus and into each of the plurality of communications terminals having encrypting capability, the information including an indication of whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption;
wherein the encryption apparatus further includes a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process is performed.
2. (Previously Presented) The system according to claim 1, wherein the encryption apparatus is configured to receive data from and retransmit the data in the form of encrypted data to one of the plurality of communications terminals having encrypting capability, and the encryption apparatus is configured to receive and retransmit the data in the form of non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability.
3. (Cancelled)

4. (Previously Presented) The system according to claim 1, wherein:
the encryption apparatus further includes a storage to store the information inputted from the manager terminal; and wherein
the encryption apparatus in performing the encrypting process and the decrypting process by is configured to compare the information stored in the storage with header information of a data packet of data received through one of the plurality of ports.
5. (Previously Presented) A system, comprising:
an encryption apparatus having a plurality of ports configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities, the encryption apparatus to perform an encrypting process or a decrypting process on data received at one of a plurality of ports after passing through a data link layer and a physical layer,
wherein the encryption apparatus is configured to output encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled; and
a manager terminal to input information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for encryption, into the encryption apparatus and those of the plurality of communications terminals having encryption capabilities, thereby completing a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data.
6. (Previously Presented) The system according to claim 5, wherein:
the encryption apparatus further includes a storage to store the information inputted from the manager terminal; and wherein

the encryption apparatus, in performing the encrypting process and the decrypting process is configured to compare the information stored in the storage with header information of a data packet of data received through one of the plurality of ports.

7. (Previously Presented) The system according to claim 1, wherein the information comprises at least one of information associated with the presence or absence of encryption or decryption process, the availability of packet communications, an encryption level, a time period to perform encryption, an encryption policy, or an encryption key.

8. (Previously Presented) The system according to claim 1, wherein the plurality of communications terminals are inside a secured network.

9. (Previously Presented) The system according to claim 1, wherein at least one of the plurality of communications terminals is outside a secured network.

10. (Previously Presented) The system according to claim 1, wherein the encryption apparatus comprises a data path for a connected terminal and wherein the encryption apparatus is configured to perform the encryption process or the decryption process on data received or transmitted on each data path using a different encryption key associated with the connected terminal.

11. (Previously Presented) The system according to claim 1, wherein the those of plurality of communications terminals having encrypting capability are connected to the encryption apparatus through an access point.

12. (Previously Presented) The system according to claim 1, wherein the plurality of communications terminals are arranged in a plurality of local area networks.

13. (Previously Presented) The according to claim 12, comprising a plurality of manager terminals, each of the plurality of manager terminals to manage encryption and decryption

settings in at least one communications terminal having the encrypting capabilities in at least one of the plurality of local area networks.

14. (Previously Presented) A method, comprising:

receiving data in an encryption apparatus configured to be connected between a plurality of communications terminals one or more having encryption capabilities and the remainder of the plurality of communications terminals having no encryption capabilities;

performing, by the encryption apparatus, an encrypting process or a decrypting process on data to terminate encryption-based security between at least one of the plurality of communications terminals having the encrypting capability and at least one of the plurality of communications terminals having no encrypting capability; and

bridging data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process, wherein

information including whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for the encryption are inputted from a manager terminal into each of the encryption apparatus and those of the plurality of communications terminals having the encrypting capability.

15. (Previously Presented) The method according to claim 14, comprising:

receiving and retransmitting, by the encryption apparatus, encrypted data from and to one of the plurality of communications terminals having the encrypting capability; and

receiving and retransmitting, by the encryption apparatus, non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability.

16. (Previously Presented) The method according to claim 14, comprising:

storing, by the encryption apparatus, information inputted from a manager terminal; and
controlling the encrypting process and the decrypting process by comparing the information stored in a storage with header information of a data packet of the data received through one of the plurality of ports.

17. (Previously Presented) The method according to claim 14, comprising:
 - performing an encrypting process or a decrypting process on data received at one of the plurality of ports after passing through a data link layer and a physical layer; and
 - outputting encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled.

18. (Previously Presented) A system, comprising:
 - a plurality of encryption apparatuses configured to be connected between a plurality of communications terminals having no encrypting capability, each of the plurality of encryption apparatuses to perform an encrypting process or a decrypting process on data to terminate encryption-based security between the communications terminals; and
 - a manager terminal for inputting information including an indication of whether or not data packets are to be discarded between specific communications terminals after the data packets have been received, and including a time period for encryption into each of the encryption apparatuses;
 - wherein each of the encryption apparatuses further include a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process.